REQUEST FORM FOR APPLICATION UNDER 37 CFR 1.53(b)

DOCKET NUMBER: 53588-025
Prior Application: U.S. Serial No. 08/901,687, filed July 28, 1997
Art Unit: 2765
Examiner: J. Campa

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

This is a Request for filing a Continuation application under 37 CFR 1.53(b) of pending prior application Serial No. 08/901,687, filed on July 28, 1997, entitled A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET, by the following named inventor(s): JOHN P. PETTITT.

1. □ I hereby state that the enclosed copy of this prior application is a true copy of the above-identified prior application.

2. Oath or Declaration
   a. □ Newly executed (original or copy)
   b. ☒ Copy from a prior application (37 CFR 1.63(d))
      i. □ Deletion of inventor(s)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

3. ☒ Incorporation By Reference (useable if Box 2b is checked)
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 2b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

4. ☒ Preliminary Amendment is enclosed.

5. ☒ An Information Disclosure Statement and PTO1449 Form are submitted herewith.

6. ☒ Cancel claims 1-16.

7. The filing fee is calculated on the basis of the claims existing in the prior application as amended at 2 and 3 above:

	NO. OF CLAIMS		EXTRA CLAIMS	RATE	AMOUNT
Total Claims	14	-20	0	$18.00 =	$0.00
Independent Claims	5	-3	2	$78.00 =	$156.00
				Basic Application Fee	$760.00
				If multiple dependent claims are presented, add $0.00	$0.00
				Total Application Fee	$916.00
				Subtract ½ if small entity	$458.00
				TOTAL APPLICATION FEE DUE	$458.00
				AMOUNT TO BE CHARGED TO DEPOSIT ACCOUNT NO. 50-0385	$458.00

7a. □ Enclosed is a Verified Statement to establish small entity status under 37 CFR 1.9 and 37 CFR 1.27.

7b. ☒ A verified Statement to establish small entity status under 37 CFR 1.9 and 37 CFR 1.27 was filed in prior application and such status is still proper and desired.

8. ☒ The Commissioner is hereby authorized to charge fees under 37 CFR 1.16 and 1.17 which may be required, including any extension of time fees to maintain the pendency of the parent application Serial No. 08/901,687 or credit any overpayment to Deposit Account No. 50-0385.

9. ☒ Amend the specification by inserting before the first line the sentence:

--This application is a continuation of Application Serial No. 08/901,687 filed July 28, 1997.--

10. □ Priority of Application Serial No. filed on , in is claimed under 35 USC 119. The certified priority document(s) were filed in Serial No. on .

11. ☒ The prior application is assigned of record to

Cybersource Corporation
San Jose, CA 95128-2545

12. ☒ The power of attorney in the prior application is to:

Stanislaus Aksman, Reg. No. 28,562; Edward A. Becker, Reg. No. 37,777; Stephen A. Becker, Reg. No. 26,527; William H. Beha, Reg. No. 38,038; Marcel K. Bingham, Reg. No. 42,327; John G. Bisbikis, Reg. No. 37,095; Kenneth L. Cage, Reg. No. 26,151; Stephen C. Carlson, Reg. No. 39,929; Paul Devinsky, Reg. No. 28,553; Laura A. Donnelly, Reg. No. 38,435; Margaret M. Duncan, Reg. No. 30,879; Brian E. Ferguson, Reg. No. 36,801; Michael F. Fogarty, Reg. No. 36,139; Wilhelm F. Gadiano, Reg. No. 37,136; Keith E. George, Reg. No. 34,111; John A. Hankins, Reg. No. 32,029; Brian D. Hickman, Reg. No. 35,894; Eric J. Kraus, Reg. No. 36,190; Edward E. Kubasiewicz, Reg. No. 30,020; Robert E. LeBlanc, Reg. No. 17,219; Jack Q. Lever, Reg. No. 28,149; Raphael V. Lupo, Reg. No. 28,363; Christine F. Martin, Reg. No. 39.762; Michael E. McCabe, Jr., Reg. No. 37,182; James H. Meadows, Reg. No. 33,965; Michael A. Messina, Reg. No. 33,424; Christopher J. Palermo, Reg. No. 42,056; Joseph H. Paquin, Jr., Reg. No. 31,647; Craig L. Plastrik, Reg. No. 41,254; Robert L. Price, Reg. No. 22,685; Paul A. Roberts, Reg. No. 40,289; Gene Z. Rubinson, Reg. No. 33,351; Joy Ann G. Serauskas, Reg. No. 27,952; Michele M. Schafer, Reg. No. 34,717; David J.

Serbin, Reg. No. 30,589; Glenn Snyder, Reg. No. 41,428; Arthur J. Steiner, Reg. No. 26,106; David L. Stewart, Reg. No. 37,578; Leonid D. Thenor, Reg. No. 39,397; Keith J. Townsend, Reg. No. 40,358; Leon R. Turkevich, Reg. No. 34,035; Christopher D. Ward, Reg. No. 41,367; Damian G. Wasserbauer, Reg. No. 34,749; Aaron Weisstuch, Reg. No. P41,557; Edward J. Wise, Reg. No. 34,523; Alexander V. Yampolsky, Reg. No. 36,324; and Robert W. Zelnick

13. ☒ Also enclosed:

4 Pages of Drawings.
Postcard.

14. □ A petition, fee and response has been filed to extend the term in the pending prior application until .

Address all future communications to: (May only be completed by applicant, or attorney or agent of record)

McDermott, Will & Emery
600 13th Street, N.W.
Washington, D.C. 20005-3096

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Christopher Pal

Christopher J. Palermo
Registration No. 42,056

600 13th Street, N.W.
Washington, DC 20005-3096
(408) 271-2300 CJP:cb
Date: November 17, 1999
Facsimile: (408) 271-2310

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL402672230US Date of Deposit 11/17/99

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

CATHY BACHMANN
(Typed or printed name of person mailing paper or fee)

Cathy Bachman
(Signature of person mailing paper or fee)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: JOHN P. PETTIT	
Serial No.: Not yet assigned	Examiner: Not Yet Assigned
Filed: Herewith	Art Unit: Not Yet Assigned
For: A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER A COMPUTER NETWORK (As amended)	

Hon. Assistant Commissioner of Patents
and Trademarks
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to examining the above-referenced application, please amend this application as indicated below.

IN THE TITLE:

Cancel the original title and insert: --A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER A COMPUTER NETWORK--.

IN THE ABSTRACT:

Line 2, change "internet" to --Internet--;

Line 9, change "internet" to --Internet--.

IN THE SPECIFICATION:

Page 1, line 5, change "internet" to --Internet--;

line 14, after “system” insert --(“AVS”)--;

line 18, change “in” to --receiving at--;

line 20, change “internet” to --Internet--; change “is” to --are--; delete “for”;

Page 2, line 2, change “as” to --in--; change “internet” to --Internet--;

line 3, change “have” to --obtain--;

line 7, change “systems” to --system--;

line 8, change “internet” to --Internet--;

line 15, before “consumer” insert --a--; change “internet” to --Internet--;

line 21, change “internet” to --Internet--;

Page 3, line 11, after “detection” insert --method, system and apparatus--;

line 12, change “internet” to --Internet--;

line 21, change “cards” to --card--; change “internet” to --Internet--;

line 23, after “includes” insert a comma;

Page 4, line 2, before “the” insert --and--; before “it” insert --information from--;

line 3, change “IVS” to --(“IVS”)--;

line 4, after “determine” insert --whether--; change “holder’s” to --information--;

line 5, change “validity” to --is valid--;

line 15, change “internet” to --Internet--;

line 18, delete "that";

line 21, change "internet" to --Internet--;

line 22, after "system" insert --("IIVS")--;

Page 5, line 3, change "one" to --IVS 106--;

line 6, after "history database" insert --222--; change "internet" to --Internet--; after "ID database" insert --224--;

line 10, delete "information"; before "database" insert --history--;

line 13, change "internet" to --Internet--;

line 14, after "system" insert --208--; after "check" insert --202--; change "internet" to --Internet--;

line 15, change "internet" to --Internet--;

line 16, change "internet" to --Internet--;

line 17, after "system" insert --208; after "check" insert --202--;

line 19, change "internet" to --Internet--;

line 20, change "internet" to --Internet--;

line 21, change "internet" to --Internet-- (two occurrences);

Page 6, line 2, after "history" insert --check 202--;

line 3, change "202 and 204" to --206--;

line 4, change "internet" to --Internet--;

line 5, change "internet" to --Internet--;

line 8, change "internet" to --Internet--;

line 10, change "internet" to --Internet--;

line 13, change "internet" to --Internet--;

line 14, change "internet" to --Internet--;

line 16, change "internet" to --Internet--;

line 18, change "internet" to --Internet--;

line 22, change "internet" to --Internet--;

line 23, change "internet" to --Internet--;

Page 7, line 1, change "care" to --card--.

IN THE CLAIMS:

Please cancel Claims 1-16 without prejudice or disclaimer, and add new Claims 17-30 as follows:

17. (New) A method for detecting fraud in a transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the method comprising the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

verifying the credit card information based upon a history check that determines whether the credit card information is consistent with the transaction information;

verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

18. (New) A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

receiving, from the merchant, transaction information that identifies the consumer and the product, including an Internet address of the consumer and a shipping address for the product;

retrieving, from the database of the Internet identification system, a plurality of records of other transaction information that are associated with the Internet address of the consumer;

determining whether a physical address contained in each of the plurality of records matches the shipping address in the transaction information;

verifying the credit card information when the physical address matches the shipping address in the transaction information.

19. (New) A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in other transaction information for other transactions associated with an Internet email address of the consumer.

20. (New) A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet identification system comprises the step of:

retrieving a plurality of records of other transactions from an Internet identification system that associates the credit card number with other physical addresses that have been specified in other transaction information for other transactions associated with an Internet address of the consumer;

creating and storing a map of the other transactions;

verifying the credit card information based upon the map of other transactions, by determining whether a physical address specified in the transaction information is consistent with the other physical addresses in the other transaction information.

21. (New) A method as recited in claim 17, further comprising the step of:

weighting each of the verifying steps according to an importance as determined by the merchant of each verifying step to the credit card transaction.

22. (New) A method as recited in claim 17, wherein the step of verifying the credit card information based upon a history check comprises the step of:

receiving, from other merchants, records of other transactions involving the other merchants and the consumer;

storing the records of other transactions in a transaction history database that can be accessed and supplemented by other merchants with information about other credit card transactions with the consumer and such other merchants;

verifying the credit card information based upon the transaction history database by determining whether the credit card information is consistent with the records of other transactions in the transaction history database.

23. (New) A method as recited in claim 17, wherein the step of verifying the credit card information based upon an Internet . identification system comprises the step of:

receiving, from other merchants, records of other transactions involving the other merchants and the consumer;

storing the records of other transactions in an Internet identification database that can be accessed and supplemented by other merchants with information about other credit card transactions with the consumer and such other merchants;

verifying the credit card information based upon the Internet identification database by determining whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in records of the Internet identification database for other transactions associated with an Internet address of the consumer.

24. (New) A method for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet comprising the steps of:

receiving, from the consumer, credit card information relating to the transaction;

creating and storing a consistency check mechanism, a transaction history check mechanism, an automatic verification mechanism and an Internet identification mechanism, each of which may indicate whether the credit card transaction is fraudulent based on transaction information, in combination with information that identifies the consumer, in which the transaction information provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent;

receiving from the merchant and storing a weight value associated with each of the mechanisms and storing the weight value in association with information that identifies the mechanisms, wherein each of the weight values signifies an importance to the merchant of the value to the credit card transaction of the associated mechanism;

weighting each value of the plurality of parameters according to the weight values;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

25. (New) A method as recited in claim 24 wherein the steps of creating and storing further include:

creating and storing a transaction history check mechanism that includes a transaction history database which can be accessed and supplemented by other merchants with information about transactions of the consumer with such other merchants.

26. (New) A method as recited in claim 24 wherein the steps of creating and storing further include:

creating and storing an Internet identification verification system (IIS) mechanism that includes an Internet address database that can be accessed and supplemented with new Internet addresses as Internet address expansion occurs.

27. (New) A method as recited in claim 24 wherein the steps of creating and storing further include:

obtaining other transactions utilizing an Internet address that is identified with the credit card transaction;

constructing a map of credit card numbers based upon the other transactions;

utilizing the map of credit card numbers to determine if the credit card transaction is valid.

28. (New) An integrated verification system for determining whether a transaction between a merchant and consumer over the Internet is fraudulent, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the system comprising:

means for receiving, from the merchant, transaction information that identifies the consumer and the product;

means for receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

means for verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

means for verifying the credit card information based upon a transaction history check that determines whether the credit card information is consistent with the transaction information;

means for verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

means for creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

29. (New) A computer readable medium containing program instructions for detecting fraud in a credit card transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, wherein execution of the program instructions by one or more processors of a computer system causes the one or more processors to carry out the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer;

verifying the credit card information based upon a transaction history check that determines whether the credit card information is consistent with the transaction information;

verifying the credit card information based upon an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

30. (New) A method for detecting fraud in a transaction between a consumer and a merchant over the Internet, wherein the transaction involves the consumer purchasing a product from the merchant using a credit card, the method comprising the steps of:

receiving, from the merchant, transaction information that identifies the consumer and the product;

receiving, from the merchant, credit card information associated with the consumer that identifies the credit card to be used in the transaction;

verifying the credit card information based upon a consistency check that determines whether the credit card information matches the consumer, a transaction history check that determines whether the credit card information is consistent with the transaction information, and an automatic verification system;

verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer;

creating and storing a fraud score value based on the verifying steps that provides the merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

REMARKS

This is a Continuation application based on Ser. No. 08/901,687, filed July 28, 1997, now allowed ("parent application"). In the parent application, Claims 1-5, 7-15, 17-19 were rejected in the Office Action mailed July 06, 1999, and these were the only rejected claims identified in that Office Action. The Applicants now address the substance of the objections and rejections of that Office Action in the context of the amended claims. No new matter is added.

ISSUES NOT BASED ON PRIOR ART

1. SPECIFICATION

The first Office Action in the parent application objected to the specification as containing grammatical errors and typographical errors. Applicant has thoroughly reviewed the specification and corrected it in this amendment. Applicant believes that all informalities have been addressed.

2. ANTECEDENT BASIS

The second Office Action of the parent application (paper number 11, mailed July 06, 1999) objected to certain claims based on lack of antecedent basis. The Applicant has carefully reviewed and amended the claims to address all antecedent basis issues.

REJECTIONS BASED ON PRIOR ART

1. CLAIM REJECTIONS - 35 U.S.C. § 103(a) (ROSE, GOPINATHAN, TOM)

Claims 1-5, 7-9 and 11-15 of the parent application were rejected under 35 U.S.C. § 103(a) as being unpatentable over ROSE (5757917) in view of GOPINATHAN (5819226) and TOM (5696907). The rejection is traversed.

As a threshold matter, Applicants respectfully suggest that the analytical approach taken by the second Office Action is legally improper. Specifically, in the discussion of former claim 1, pages 6-8 of the second Office Action argue that individual steps or features of the claims are obvious. This is improper. The correct approach addresses the combination recited in the claim as a whole, Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983); MPEP § 2141.02. The Office Action may not pick and choose elements of the claimed combination, assert that any individual element would have been obvious, and then reject the claimed combination as obvious, absent a teaching or suggestion in the art to create the entire combination of the claim as a whole.

The new claims recites a method and system providing distinct improvement over AVS systems. Independent Claims 17, 24, 28, 29, and 30 feature, among other things, verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer.

The second Office Action of the parent application addressed this feature in the context of former Claim 2. Specifically, the Office Action contended that TOM discloses "an Internet identification system parameter" in the form of "residence stability." This is incorrect and appears to reflect a misunderstanding of the meaning of "Internet identification system."

Each of the new independent claims features verifying the credit card information based upon an Internet identification system that determines whether a physical address specified in the transaction information is consistent with other physical addresses that have been specified in a database of records of other transaction information for other transactions that are associated with the Internet address of the consumer. TOM's concept of "residence stability" is not the "Internet identification system" as claimed. TOM's teaching of "residence stability," at best, suggests a determination of whether a loan applicant is transient, i.e., the applicant has had multiple residence addresses in a short period of time. This is a completely different concept from that of the independent claims - i.e., whether the consumer has given different "ship-to" addresses in past Internet transactions, as indicated by information that is associated with the consumer's Internet address, e.g., an email address, IP address, or other unique online identifier.

With regard to former Claim 1, the Office Action states:

> "[TOM] teaches: - each of the transaction values being weighted according to an importance, as determined by the merchant or from past experience, of that value to the credit card transaction, so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent (see column 5, lines 24-67 and column 6, lines 1-46; Figure 7, a neural network is used to provide risk and credit evaluations of newly proposed financial service applications based upon a plurality of parameters which are weighted according to the information contained therein). ... It would have been obvious to one having ordinary skill in the computer and business arts at the time of applicant's invention to combine the teachings found in Rose and Gopinathan et al. with Tom's teachings, which shows weighting various parameters in an instant credit application based upon a credit manager's past experience to provide indications of credit worthiness for purposes of evaluating financial service applications. One having ordinary skill in the computer and business arts at the time of applicant's invention would have been motivated to combine the ... teachings to get the advantage of placing a greater significance upon certain weights over others in verifying whether an instant credit card transaction is fraudulent...."

Applicant disagrees. The argument glosses over differences between the claimed invention and the teachings of the references. The "parameters" in TOM are different from the parameters of the present application. TOM describes weighting nodes of a neural network in which each node corresponds to a value of a variable that describes the consumer. In contrast, the weighting parameters that are disclosed and claimed by Applicant are different classes of tests or checks rather than individual variable values.

In Applicant's disclosure, a "parameter" is a test or check, not a scalar value. This usage may be unconventional, which is permitted, and it is not the same usage as TOM.

Further, risk and credit evaluations of newly proposed financial service applications, or "instant credit applications," as described in TOM, are not the same as fraud detection in a credit card transaction. Risk and credit evaluations involve determining the creditworthiness of an applicant for a loan or other financial service. For example, such evaluations may determine whether the consumer has sufficient available credit to complete a desired transaction. In contrast, fraud detection involves determining whether a consumer offering a credit card number is not actually the cardholder. Applicant has discovered that fraud detection can be carried out effectively based on external transaction information rather than information describing the consumer, including the consumer's amount of available credit. The risk and credit evaluations contemplated by TOM do not involve a loan applicant falsifying his or her identity. In short, TOM addresses a different problem and is improperly combined with ROSE and GOPINATHAN.

Moreover, the claimed invention does not involve verifying whether "an instant credit card transaction" is fraudulent. The Office Action appears to coin this term in order to suggest an association of the claimed invention and TOM. This terminology is incorrect and not used in the specification or claims.

Claim 18 elaborates on the Internet identification system feature of Claim 17 by specifically reciting a particular mechanism for obtaining the Internet identification information, and determining whether a physical address contained in each of the plurality of records matches the shipping address in the transaction information. This specific comparison is not shown in the art of record.

Claim 19 specifically features use of the consumer's email address as one kind of identification element in the Internet identification system. The combination of steps in Claim 19 is not taught or suggested by the art of record.

Claim 20 specifically features use of a map of other transactions in combination with the steps of Claim 17. A similar feature was found allowable in the parent application.

Claim 21 features weighting each of the verifying steps <u>according to an imporance as determined by the merchant</u> of each verifying step. For the reasons given above with respect to the weighting feature of former claim 1, Claim 21 is allowable.

Claim 22 features receiving records of other transactions <u>from other merchants</u> and updating the transaction history database accordingly. The shared database feature of Claim 22 is not found in the art of record. The Office Action addresses this feature in the context of former Claim 3 and Claim 4, and argues official notice. Reliance on official notice is improper because the subject matter of the official notice is not "capable of instant and unquestionable demonstration as being 'well-known' in the art," see MPEP § 2144.03. Applicant requests the Office to cite a specific reference to substantiate the basis for the official notice. Conventional practice is for a merchant to secure its own database and prevent third parties, including other merchants, from adding to it. Conventional practice is for the merchant to look only in its own database for records of past transactions with the same consumer.

Claim 23 features receiving records from other merchants and updating the Internet identification system database. The shared database feature of Claim 23 is not found in the art of record.

Each of new claims 24-30 features one or more of the foregoing features and is believed to be allowable for the corresponding reasons set forth above.

Specifically, Claim 24 recites use of a consistency check mechanism, transaction history check mechanism, automatic verification system, and the Internet identification system. The Office Action asserts that TOM teaches such features, however, TOM does not teach a consistency check parameter which is used to determine whether the credit card information is consistent. TOM teaches analysis of information including residence stability. In contrast, Applicant discloses and claims a consistency check parameter, which allows one to determine whether the credit information is consistent, i.e., does the credit information match the user. See Specification at page 5. Residence stability information (whether a consumer has several different past addresses) is not the same as testing whether the credit information supplied by the consumer matches the consumer.

TOM does not teach a history check parameter. TOM describes considering credit history information. However, the claimed transaction history check is not credit history information; it is information about prior transactions carried out by the same consumer.

TOM does not teach an Internet identification system parameter as claimed. The Office Action suggests that the "residence stability" information of TOM is an Internet identification system parameter, but information about whether a consumer has had multiple residence addresses in a short period of time is not the same as determining whether the same credit card is being used by a consumer claiming several different Internet addresses.

Claim 24 includes an automatic verification system mechanism. Addressing canceled Claim 2, the Office Action states that an automatic verification system parameter is obvious and that applicant admits it is prior art.

Applicant disagrees. Admitting that a particular element is known in the art is not an admission that a combination of that element with others would have been obvious. Carrying out credit card verification, through manual observation or use of an AVS system, is old. But the selection and use of an AVS system, in combination with particular parameters that represent external factors, or information in combination with consumer-identifying information, is not shown in the art of record. There is no suggestion in the art of record to combine an AVS system with the teachings of the cited art.

For the reasons given above, the new claims are believed to be in allowable condition in light of the art of record.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is respectfully requested.

The Examiner may contact the undersigned by telephone if such contact would further the examination of the present application.

Petition for Extension: Applicant hereby petitions, under 37 C.F.R. 1.136, for such extensions of time as may be necessary to cause this Preliminary Amendment and the associated Continuation application to be timely on the filing date granted to it by the Office.

The Commissioner is authorized to charge any fees due in connection with this response, and to credit any overpayment to

Deposit Account No. 50-0385. A duplicate of this paper is filed herewith.

Respectfully submitted,

McDERMOTT, WILL & EMERY

Date: November 17, 1999

Christopher J. Palermo
Reg. No. 42,056

(408) 271-2300
600 13th Street, N.W.
Washington, D.C. 20005

A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET

FIELD OF THE INVENTION

The present invention relates generally to credit card transactions and specifically to detecting fraud in such credit card transactions when ordering and downloading information over the internet.

BACKGROUND OF THE INVENTION

Credit card transactions are being utilized in a variety of environments. In a typical environment a user provides a merchant with a credit card, and the merchant through various means will verify whether that information is accurate. For example, referring now to Figure 1, a typical credit card verification system 10 is shown. In such a system, a merchant 12 receives a credit card from the customer 14. The merchant then verifies the credit card information through an automated verification system 16.

These systems work well in a credit card transaction in which either the customer has a face-to-face meeting with the merchant or the merchant is actually shipping a package or the like to the address of a customer. The verification procedure typically includes in the AVS system address information and identity information. However, when downloading information from an online service or the internet, the address and identity information is not enough for to adequately verify that the customer who is purchasing the goods is actually the owner of the credit card. For example, an individual may have both the name and the address of a particular credit card holder and that information in a normal transaction may be sufficient for authorization of such a transaction. However, as an internet transaction it is possible to have all the correct information related to the particular credit card holder through unscrupulous means, and therefore, be able to fraudulently obtain information.

Accordingly, what is needed is a system and method that overcomes the problems associated with a typical verification systems for credit card transactions particularly in the internet or online services environment. The system should be easily implemented within the existing environment and should also be straightforwardly applied to existing technology. The present invention addresses such a need.

SUMMARY

A method and system for detecting fraud in a credit card transaction between consumer and a merchant over the internet. The method and system comprises obtaining credit card information relating to the transaction from the consumer; and verifying the credit card information based upon a variety of parameters. The variety of parameters are weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. In so doing, an integrated verification system is provided which allows a merchant, or the like, to accurately and efficiently determine the validity of a transaction over the internet.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is diagram of the prior art verification system for credit card transaction.

Figure 2 is a verification system in accordance with the present invention.

Figure 3 is a flow chart of the verification system in accordance with the present invention.

Figure 4 is a flow chart of the integrated verification system in accordance with the present invention.

DETAILED DESCRIPTION

The present invention relates to a fraud detection for use in credit card transaction over online services or the internet. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein.

The present invention provides an integrated verification system for credit cards transactions over an online service or the internet. Referring now to Figure 2, what is shown is a block diagram of a system 100 which would use the verification procedure in accordance with the present invention. System 100 includes similar to

Figure 1, a customer 102 and a merchant 104. The customer 102 provides the merchant with a credit card, the merchant then sends it to an integrated verification system IVS 106 which includes a variety of parameters providing consistency, history and other information in an integrated fashion to determine the credit card holder's validity. The IVS 106 is typically implemented in software for example in a hard disk, floppy disk or other computer-readable medium. In a typical embodiment, when the customer 102 orders a particular piece of software to be downloaded from a merchant 104, the merchant will provide the credit card number, e-mail address and other pertinent information to the IVS 106. The integrated verification system 106 then weights the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent. To more clearly describe the operation of a system and method in accordance with the present invention, refer now to the following discussion in conjunction with the accompanying figures.

Figure 3 shows a simple block diagram for providing an integrated verification of a credit card transaction over the internet. The IVS 106 includes a controller 212 which receives the credit information from the merchant and then sends that information on to a variety of parameters 202-208. The plurality of parameters that operate on the information to provide an indication of whether the transaction is valid. In this embodiment, the plurality of parameters comprises a history check 202, a consistency check 204, an automatic verification system 206 and an internet identification verification system 208. The output or individual indications of validity of these parameters are provided to fraud detector 210. The fraud detector 210 combines these inputs to provide an integrated indication of whether the particular transaction is valid.

Consistency check 204 allows one to determine whether the credit information is consistent, i.e., does the credit information match the user and other information. AVS system 206 provides similar information as AVS 16 described in Figure 1. A key feature of both the history database and the internet ID database is that they can be accessed and the information there within can be supplemented by a variety of other merchants and, therefore, information from those merchants is obtainable thereby.

History information check 202 is provided which also accesses a database 222 which may include card number and email information. The history check 202 will also actively determine if the particular transaction matches previous database information within the history database 222. Therefore, the internet ID verification system and history check increases in utility over time. The internet ID verification system 208 provides for a system for verifying the validity of an internet address, the details of which will be discussed hereinafter. The internet identification verification system similar to the history check includes a database 224 which can be added to by other merchants.

In addition, the internet identification verification system 208 accesses and communicates with a database of internet addresses. This system will be used to verify whether the internet address is consistent with other internet addresses being used in transactions utilizing this credit card.

These different parameters are weighted via weighting blocks 214-220, respectively, dependent upon the particular credit card transaction. For example, if the amount of dollar transaction is critical, it may be appropriate for the history and AVS system 202 and 204 to be weighted more critically than the other parameters. On the other hand, if a critical point is the consistency of the internet address, then the consistency check 204 and the internet identification system 208 may be more critical. Accordingly, each of the verification parameters 202-208 may be weighted in different amounts depending upon its importance in the verification process.

A particularly important feature of the present invention is the internet identification system 208 and its operation within the integrated verification system 106. Through this system 208, it is possible to quickly determine if an internet identification address is being utilized fraudulently. To describe this feature in more detail, refer now to Figure 4 and the accompanying discussion.

Figure 4 is a flow chart of the internet identification verification system **208**. The goal of internet identification verification system 208 is to determine whether the physical address or the physical location of the address compares to a previous physical location that was used for that particular internet address. Accordingly, in the flow chart of Figure 4, first the number of transactions that had been processed using that particular internet address is obtained from the database 224, via step 302. Thereafter, a map of those transactions is constructed based on those obtained transactions, via step 304. Finally, the constructed map is used to determine if the new credit card transaction is valid, via step 306. Accordingly, through a system and method in accordance with this system, an internet identification verification system is provided which can quickly and easily determine whether a particular internet address is related to a particular credit care transaction.

Accordingly, what is provided is a system and method for accurately determining whether a particular credit card transaction is a fraudulent one. The integrated verification system in accordance with the present invention provides for weighting the variety of parameters so as to provide a merchant with a quantifiable indication on whether the credit and transaction is fraudulent.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will recognize that there could be variations to the embodiment and those variations would be within the spirit and scope of the present invention. Therefore, although the present invention was described in terms of a particular verification system, one of ordinary skill in the art readily recognizes, that any number of parameters can be utilized and their use would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill without departing from the spirit and scope of the present invention, the scope of which is defined by the following claims.

CLAIMS

What is claimed is:

1. A method for detecting fraud in a credit card transaction between consumer and a merchant over the internet comprising the steps of:

a) obtaining credit card information relating to the transaction from the consumer; and

b) verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

2. The method of claim 1 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

3. The method of claim 2 wherein the history check includes a database which can be accessed and supplemented by other merchants.

4. The method of claim 2 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

5. An integrated verification system for determining credit card transactions between a merchant and consumer over the internet are fraudulent, the system comprising:

a controller for receiving credit card transaction information;

a plurality of parameters for receiving the transaction information from the controller means and for providing individual indications of the validity of transactions;

and detector means for receiving the indications of validity and providing an integrated indication of validity.

6. The system of claim 5 wherein each of the plurality of parameters includes a weighting factor.

7. The system of claim 5 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

8. The system of claim 7 wherein the history check includes a database which can be accessed and supplemented by other merchants.

9. The system of claim 7 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

10. A method for verifying the validity of a credit card transaction over the internet comprising the steps of:

a) obtaining other transactions utilizing an internet address that is identified with the credit card transaction; , weighting

b) constructing a map of credit card numbers based upon the other transactions and; other merchants

c) utilizing mapped transactions to determine if the credit card transaction is valid.

11. A system for detecting fraud in a credit card transaction between consumer and a merchant over the internet comprising:

means for obtaining credit card information relating to the transaction from the consumer; and means for verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit care transaction is fraudulent.

12. The system of claim 11 wherein the plurality of parameters include a consistency check, a history check, an automatic verification system and an internet identification system.

13. The system of claim 12 wherein the history check includes a database which can be accessed and supplemented by other merchants.

14. The system of claim 12 wherein the internet identification system includes a database which can be accessed and supplemented by other merchants.

15. A computer readable containing program instructions for detecting fraud in a credit card transaction between consumer and a merchant over the internet, the program instructions:

a) obtaining credit card information relating to the transaction from the consumer; and

b) verifying the credit card information based upon a plurality of parameters; the plurality of parameters being weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent.

16. A computer readable medium containing program instructions for verifying the validity of a credit card transaction over the internet, the program instructions:

a) obtaining other transactions utilizing an internet address that is identified with the credit card transaction;

b) constructing a map of credit card numbers based upon the other transactions and;

c) utilizing mapped transactions to determine if the credit card transaction is valid.

ABSTRACT

A method and system for detecting fraud in a credit card transaction between consumer and a merchant over the internet. The method and system comprises obtaining credit card information relating to the transaction from the consumer; and verifying the credit card information based upon a variety of parameters. The variety of parameters are weighted so as to provide a merchant with a quantifiable indication of whether the credit card transaction is fraudulent. In so doing, an integrated verification system is provided which allows a merchant, or the like, to accurately and efficiently determine the validity of a transaction over the internet.

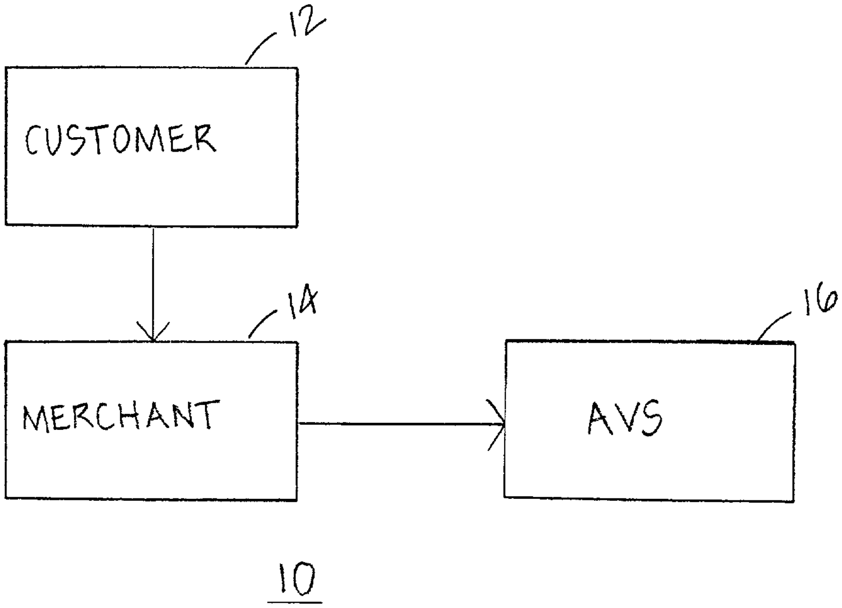

FIG. 1

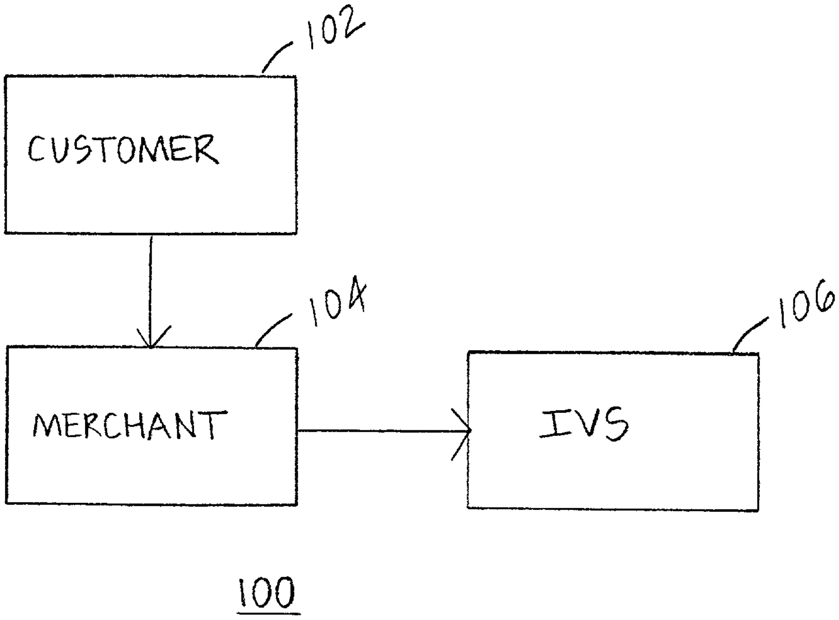

FIG. 2

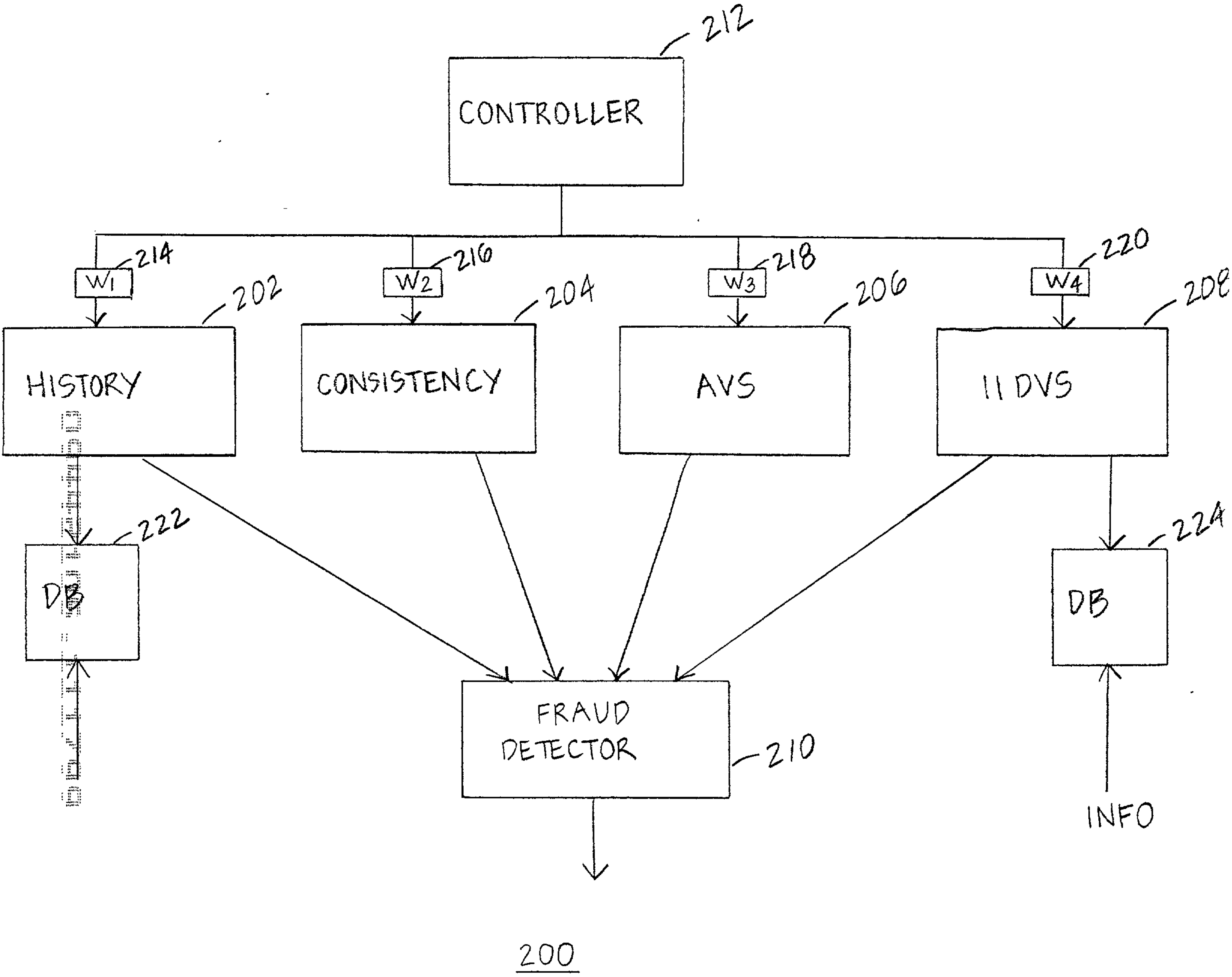
212
CONTROLLER
W1
214
W2
216
W3
218
W4
220
202
HISTORY
204
CONSISTENCY
206
AVS
208
II DVS
222
DB
224
DB
FRAUD DETECTOR
210
INFO
200

FIG. 3

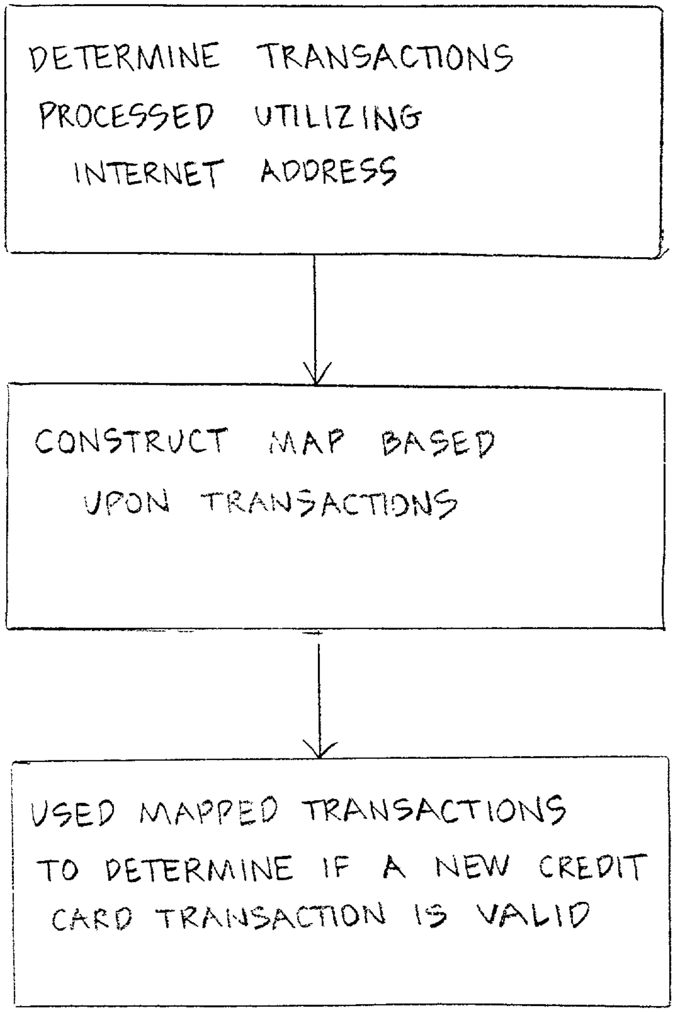
DETERMINE TRANSACTIONS PROCESSED UTILIZING INTERNET ADDRESS
CONSTRUCT MAP BASED UPON TRANSACTIONS
USED MAPPED TRANSACTIONS TO DETERMINE IF A NEW CREDIT CARD TRANSACTION IS VALID

FIG. 4

DECLARATION

As the below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name; and that I verily believe I am the original, first and sole inventor of the invention entitled:

A METHOD AND SYSTEM FOR DETECTING FRAUD IN A CREDIT CARD TRANSACTION OVER THE INTERNET

described and claimed in the specification which is attached hereto that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that I do not know and do not believe the same was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application, that I acknowledge my duty to disclose information of which I am aware which is material to the examination of this application, and that no application for patent or inventor's certificate on said invention has been filed in any country foreign to the United States of America by me or my legal representatives or assigns.

Address all telephone calls to Mr. Sawyer at telephone number (415) 493-4540 and all correspondence to:

Joseph A. Sawyer Jr.
SAWYER & ASSOCIATES
620 Hansen Way, Suite A
Palo Alto, California 94304

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such wilful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of sole or
First Inventor: **John Philip Pettitt**

Residence: **650 Palm Avenue**
Los Altos, California 94022

Post Office Address:	**650 Palm Avenue**			
	Los Altos	**Santa Clara**	**CA**	**94022**
	City	County	State	Zip

Citizenship: **U.K.**

7/24/97
Date

Signature

EXPRESS MAIL NO.
EL 402612230US

Attorney Docket: JAS 545P

RECORDATION FORM COVER SHEET
PATENTS ONLY

US Department of Commerce
Patent & Trademark Office

To the Assistant Commissioner for Patents: Please record the attached original documents:

1. Name of conveying party(ies):

John Philip Pettitt

Additional name(s) of conveying party(ies) attached: Yes___ No XX

2. Name and address of receiving party(ies):

Name: **Cybersource Corporation**

Street Address: **550 S. Winchester Blvd.**
Suite 301

City: **San Jose** State: **CA** ZIP: **95128-2545**

Additional name(s) & address(es) attached?
___ Yes XX No

3. Nature of conveyance:

XX Assignment

Execution Date: July 24, 1997

4. Application number(s) or patent number(s):

If this document is being filed together with a new application, the execution date of the application is: July 24, 1997.

A. Patent Application No.(s)

B. Patent No.(s)

Additional numbers attached? _Yes XX No

5. Name and address of party to whom correspondence concerning document should be mailed:

Name: **Joseph A. Sawyer, Jr.**
Internal
Address: **Sawyer & Associates**
Street
Address: **620 Hansen Way, Suite A**
Palo Alto, California 94304

6. Total Number of applications and patents involved: **One**

7. Total fee (37 CFR 3.41).........$ **40.00**
___ Enclosed
XX Authorized to be charged to deposit account

8. Deposit Account Number: 02-2120
(Attach copy of this page)

9. Statement and signature.

To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.

Joseph A. Sawyer, Jr.

7/28/97
Date

Total number of pages including cover sheet, attachments, and document: 2